JOURNAL *of*
EXTREME ANTHROPOLOGY

ISSN: 2535-3241 Vol. 4, No. 1 (2020): 45-73 https://doi.org/10.5617/jea.7813

Article

Imposter Paranoia in the Age of Intelligent Surveillance

Policing Outlaws, Borders and Undercover Agents

Tereza Østbø Kuldova
OsloMet – Oslo Metropolitan University

Abstract

Artificial intelligence, deep learning and big data analytics are viewed as the technologies of the future, capable of delivering expert intelligence decisions, risk assessments and predictions within milliseconds. In a world of fakes, they promise to deliver 'hard facts' and data-driven 'truth', but their solutions resurrect ideologies of purity, embrace bogus science reminiscent of the likes of anthropometry, and create a deeply paranoid world where the Other is increasingly perceived either as a threat or as a potential imposter, or both. *Social sorting* in the age of intelligent surveillance acquires a whole new meaning. This article explores the possible effects of *algorithmic governance* on society through a critical analysis of the figure of the imposter in the age of intelligent surveillance. It links a critical analysis of new technologies of surveillance, policing and border control, to the extreme ethnographic example of paranoia within outlaw motorcycle clubs – organizations that are heavily targeted by new and old modes of policing and surveillance, while themselves increasingly embracing the very same logic and technologies themselves. With profound consequences. The article shows how in the quest for power, order, profit, and control, we are sacrificing critical reason and risk becoming as a society not unlike the paranoid criminal organizations.

Keywords

Imposter, paranoia, fear, artificial intelligence, surveillance, outlaw motorcycle clubs, risk society

> Whoever fights monsters should see to it that in the process he does not become a monster.
>
> **— Nietzsche**

Introduction

Social bots, spies, deep fakes, undercover agents, document fraud, cyberfraudsters, fake news, fake science, counterfeits, imposters, fakes profiles, scammers, propaganda, spam, lies, con artists, hoaxes, disinformation and deception. In the digital era of *surveillance capitalism* (Zuboff 2019), the sources and means of deception and make-believe proliferate as do the means of *social sorting, targeting,* and *profiling* (Bauman & Lyon 2013). They are creating a world where distinguishing between the fake and the real, truth and lie, machine and human, becomes increasingly difficult, if not impossible. A world where making these distinctions becomes an obsessive preoccupation – a preoccupation that replaces critical thinking with fact-checking, Truth-O-Meters, and audits, openness with borders and gates, trust with transparency and control, and the politics of citizenship with identity management (Muller 2009). This obsession in turn generates new forms of harm and injustices as it sacrifices privacy, rights, liberties, the presumption of innocence, and due process on the altar of security (Benjamin 2019; O'Neil 2016) – and with it, more often than not, security itself. They are creating a world where the omnipresent corporate and governmental surveillance (the two increasingly blurred) and the continual manufacturing and mediatization of new threats, risks, and fear feeds societal paranoia, generalized suspicion and mistrust (Frosh 2016; Breton). Everyone is a potential imposter, fraud or fake; nobody can be trusted. Distrust is institutionalized (Whelan 2013).

Contemporary forms of paranoia and mistrust are related to the prevailing sense of the inability to tell truth from lie, to the feeling of overwhelming complexity and confusion, to the constant bombardment with pieces of data and information that lack any coherent frame and meta-narrative, to the persistent sense of being tracked, observed and monitored, and thus to the general post-modern feeling of a world spinning out of control (Lyotard 1984) – a feeling I have encountered among my informants from within the outlaw motorcycle subculture. Paranoia in this sense is 'a representation of the state of the psychosocial subject under conditions in which it is very hard to trust, or even to understand, what is going on around us' (Frosh 2016: 14). The increasing popularity of conspiracy theories in a surveillance society is not coincidental; belief in conspiracy theories is precisely related to this sense of confusion, disorder, paranoia, and to the normalization of surveillance (Harper 2008; Holm 2009; Wahl-Jorgensen, Bennett, & Cable 2016). As Frederik Jameson once remarked,

> conspiracy, one is tempted to say, is the poor person's cognitive mapping of the postmodern age; it is a degraded figure of the total logic of late capital, a desperate attempt to represent the latter's system, whose failure is marked by its slippage into sheer theme and content (Jameson 1988: 356).

The neoliberal 'depoliticizing machinery of fear and consumption' (Giroux 2015: 108) generates ever new threats, risks, and fears (Furedi 2002; Linke & Smith 2009), parallel to ever new pleasures, desires and 'ethical' products that promise to

relieve the very anxiety that this machinery creates (Kuldova 2018a). But this machinery, obsessed in equal measure with security and consumption, also produces another range of products for both private and governmental use: products that promise to protect us from threats and imposters, while simultaneously feeding paranoia, mistrust and fear. These products, to use a materialist perspective (Althusser 1971), can be seen as the very embodiment and expression of the ruling societal ideologies; they *do* something to us – they fundamentally transform the ways in which we relate to each other and perceive the Other and as such they are instrumental in new forms of social ordering.

In this contribution, I will try to capture some of these transformations and the resulting 'imposter paranoia'. Firstly, I invite the reader to take a closer look at the contemporary figure of the imposter in relation to 'algorithmic governance' and new technologies that facilitate the expansion of the logic of *social sorting* and *profiling* into ever new realms of social life (Katzenbach & Ulbricht 2019). This will allow us to place the ethnographic example into a larger context of societal and technological development that can be in many ways considered global. Consequently, I turn to the case of *outlaw motorcycle clubs* (OMCs) in Central Europe, linking my analytical perspectives to ethnographic material collected in Germany and through digital ethnography.[1]

Before we turn to the first part of my argument, let me set the stage for the consequent reading of the effects of algorithmic governance through the case of the outlaw bikers. This will allow us to think through the socio-technological context while keeping the key elements of the subculture in mind. I will try to show that thinking the 'imposter' through outlaw motorcycle clubs, such as the most notorious Hells Angels MC (est. 1948)[2], can offer illuminating insights into the dynamics of imposter paranoia in the age of intelligent surveillance. Unlike ordinary Harley Davidson clubs and riders, the transnational brotherhoods of outlaw motorcycle clubs are known for their involvement in the drug trade, prostitution, illegal weapons, and increasingly cybercrime, and are considered organized crime groups by law enforcement agencies across the globe. These clubs are represented in the media, by politicians and law enforcement as an increasing threat to public safety.

---

[1] This article builds on ethnographic fieldworks and other material collected between 2016-2018 in Germany, Austria, Czech Republic and Slovakia, and a research project *Gangs, Brands and Intellectual Property Rights: Interdisciplinary Comparative Study of Outlaw Motorcycle Clubs and Luxury Brands*, provided by the Research Council of Norway through a FRIPRO Mobility Grant, contract no 250716 (the FRIPRO Mobility grant scheme (FRICON) is co-funded by the European Union's Seventh Framework Programme for research, technological development, and demonstration under Marie Curie grant agreement no 608695). In this article, I do not wish to go in depth into this material, as results from this project, which is now concluded have been published elsewhere, but I wish to utilize some of the observations to make a larger, and more general point. For more details on this research, please consult the following publications: (Kuldova 2017a, 2017b, 2018d, 2018e, 2018c, 2019a, 2019b, 2020; Kuldova & Sánchez-Jankowski 2018).

[2] Today, only the Hells Angels have more than 450 charters in over 50 countries and have established themselves as a corporation and; other transnational outlaw motorcycle clubs such as Bandidos MC, Gremium MC, Mongols MC and others have followed the HAMC business model (Kuldova 2017a).

Their heavily mediated crimes merge smoothly with their intimidating aesthetics and pop-cultural representations, their reputation and their 'criminal capital' (Sandberg & Shammas 2015); together they create the perfect public enemy: transnational, 'barbarian', ruthless, driven by honour and greed – or at least this is how the threat they represent is presented to the public (Kuldova 2019c; Kuldova & Quinn 2018). The clubs are precisely one of the threats we are meant to fear; as such, they are instrumental to the widespread politics of fear, or else the 'decision makers' promotion and use of audience beliefs and assumptions about danger, risk, and fear, to achieve certain goals' (Altheide 2006: 415). Due to their intimidating appearance, and reputation, they are a straightforward *target*: they present a visible *risk* that is easy to *profile*. As such, the OMCs are actively used to legitimize new security measures, the expansion of law enforcement powers and the pre-emptive targeting of *groups*, raising concerns about civil liberties and the rule of law (Morgan, Dagistanli, & Martin 2010; Kuldova 2018c). Their transnational activity (and the activities of similar organizations) is used to legitimize increased data and intelligence sharing, cross-agency and international collaboration; their crimes legitimize the very existence of agencies such as EUROPOL.[3] Indeed, there is no doubt that outlaw motorcycle clubs have been connected to a range of crimes, which the clubs do not deny either, but it is equally no doubt that their crimes are simultaneously strategically used to legitimize legal changes, undercover surveillance, network and social media analysis, and the use of predictive policing tools that would most likely raise eyebrows of the public and civil society if used indiscriminately against the whole population. And yet, this is precisely what the use of legitimation through exceptional and extraordinary cases enables. The clubs may have a point, even if we may have little sympathy for them, when they reiterate: first they target us and then everyone else, it is everybody's civil liberties that are at stake here. And while they have a point here, they use this point for what it is worth: as I have shown in detail elsewhere, they skillfully position themselves both as victims and as justice warriors and civil rights defenders in order to recruit supporters, gain new members and mobilize anti-establishment resentment to their advantage (Kuldova 2019b, 2019c). In many places, especially in marginalized localities hit by neoliberal restructuring of society, they are succeeding at that. We may have a problem when outlaw motorcycle clubs appear more trustworthy than the political establishment.

Outlaw motorcycle clubs are much more than gangs offering their members access to the illegal economy; they are complex social institutions, closed but transnationally networked male-only groups that offer their members belonging, purpose, mission, meaning, and, as I have argued at length elsewhere, experiences of sovereignty, control, symbolic immortality, the sacred and something worth sacrificing oneself for, namely the brotherhood (Kuldova 2019b). In a chaotic and complex world, they offer a clear, straightforward narrative that explains the world to their

---

3 https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/outlaw-motorcycle-gangs (accessed 21 January 2020).

members, one accompanied by powerful rituals and rules that structure their everyday life. But there is a price to pay for meaning, and orientation, and for living with 'real', trustworthy, brothers – members of the club that have proven their identity, and commitment. The clubs are 'greedy institutions' (Coser 1974); the price for meaning, structure, control and sovereignty is – paradoxically –total submission to the organization; a greedy institution demands undivided commitment, it demands to be everything to the individual who is expected to define his whole being and identity through this institution. The *authentic* self is to be fully in line, even *identical* with the institution, one that is shaped according to its values and crafted by its routines, rituals and demands.

The clubs, being closed and secretive, depend for their continued existence and growth on the one hand on policing of their social borders, and on attracting new potential members, growing their 'brand' reputation, and gaining supporters, on the other. The clubs produce their own merchandize, organize biker events and tattoo fairs, promote themselves at Harley Davidson and other biker events, and actively commodify their own 'power mystique' (Kuldova 2017b). At the same time, they have to protect their boundaries and their secrets. The balancing game is one of *self-commodification* for the outsiders and simultaneous *securitization* of the inside, of the sacred core where the power of the organization resides. This securitization of the clubs within the context of intense commodification translates into policing of the boundaries of the club against its penetration of imposters and against the dilution of its power mystique. This logic of simultaneous securitization and commodification, as I will try to show, is not unique. Within this scenario, undercover agents are as threatening as those dressing up in counterfeit patches or companies appropriating their trademarked (and to the clubs sacred) logos in their products and 'diluting' their brand (for extensive detail on this, see: Kuldova 2017a). On the one hand, outlaw motorcycle clubs have become pop cultural heroes and subcultural icons – immortalized in movies such as *The Wild One* (Benedek 1953) or TV shows such as *Sons of Anarchy* (Sutter 2008-2014). Their real-world reputation for crime and all manners of transgression combined with the spectacular mediated images has over time built their 'power mystique' (Kuldova 2017b), attracting new members across the globe. On the other hand, much like nation states, criminal organizations (albeit transnational) are in the business of protection. They struggle to act as sovereign agents – both in the sense of Schmitt and Bataille (Schmitt 2007; Bataille 1993); they screen the identity of the members, ensure a high-level of homogeneity within their value brotherhood, and police their borders. The clubs depend on carefully screening any prospective members; they conduct background checks, credibility tests, use hackers, informants and surveillance technologies to eliminate potential threats and imposters. Anyone wanting to join the club has to prove themselves over a long period, first as a hang-around and then as a prospect; only then can he be ritually included and initiated in the brotherhood, receive his patch, his new identity, and be reborn as a member of an outlaw motorcycle club (Thompson 2012). This peculiar blend of the need to commodify the subculture in order to grow, while protecting its borders by making a sharp distinction between insiders (members) and outsider

(be they supporters or 'citizens'), means that the subculture is both *commodified* and *securitized* (by both external and internal actors).

Hence, labelled as organized crime groups by law enforcement agencies worldwide, while glamorized in popular culture, outlaw motorcycle clubs are equally paranoid of undercover agents and covert surveillance, as they are of those they see as wannabe bikers trying to make it inside the clubs (Thompson 2008). The stories of undercover agents penetrating notorious outlaw motorcycle clubs such as Joe Dobyns or William Queen (Dobyns 2010; Queen 2011) have become as notorious as the movies, books and TV series inspired by the real outlaws – both in turn shaping the realities on ground, as the real tries to live up to the imaginary. Subject to heavy surveillance, profiling and targeting, as well as social media intelligence (SOCMINT) – no less due to their 'visibly deviant' appearance, outlaw motorcycle clubs have become deeply *paranoid subcultures*, utilizing the very same technologies of surveillance that are used against them, against outsiders as well as their own. They are not only watched and intercepted, but they watch their own: control and mistrust increasingly lurk behind the rhetoric of trust, love and brotherhood. At the same time, there is an internal resistance to the logic of surveillance to which they are exposed. The clubs are increasingly engaged in mobilizing anti-establishment resentment (using social media skillfully to target potential supporters) (Kuldova 2019c), advancing conspiracy theories online and within their milieu, and even organizing popular demonstrations against the security state, excessive surveillance of citizens and disproportionate targeting, defending fundamental rights, right to privacy, due process and the presumption of innocence against a system that is becoming increasingly predicated on the presumption of guilt until proven otherwise; a system turned on its head (Kuldova 2018c; Lindenmuth 2019).

In this article, I think the clubs through the lens of the impostor and intelligent surveillance in order to point to a more general transformation where two concepts emerge as particularly significant: authenticity and paranoia. The clubs thus present a case in point, an extreme one, of a possible societal response to the use of these technologies of surveillance and policing. While I have touched both upon authenticity and paranoia, the security state and surveillance in relation to the outlaw motorcycle subculture earlier (Kuldova 2019b), here I shall attempt to think the clubs through the lens of the imposter and in relation to the latest technological developments in intelligent surveillance and artificial intelligence (AI) predictive analytics increasingly used in policing and border control – that increasingly permeates the general logic of boundary making and maintenance. I will try to show how policing of crime facilitated by the use of these technologies increasingly collapses into *policing* of social boundaries and social sorting, and the reverse. Both processes are dominated by the logic of *risk* – by the colonization of societal institutions by the culture of risk management in the context of uncertainty (Beck 1992; Power 2004; Rothstein, Huber, & Gaskell 2006) and by an uncanny obsession with *authenticity* that is both commodified and securitized.

Artificial Intelligence, Surveillance, and Social Sorting

The contemporary paranoia of the imposter, of the 'wolf in sheep's clothing', comes in many guises: the refugee with a fabricated story – most notoriously the 'imposter children' (Silverman 2016), the welfare fraudster, the terrorist, fake followers, social bots impostering as humans, predatory journals, phishing emails, imposter websites, identity thieves. The more our societies are being shaped by tech giants, technocratic pseudo-politics, securitization, and *algorithmic governance* reliant on 'big data' (Campbell-Verduyn, Goguen, & Porter 2017; Mbadiwe 2018; Valentine 2019; Hallsworth & Lea 2011), the more we tend to look to the same 'hard data' as an omnipotent source of the truth. The knowledge that informs decisions today is witnessing a fundamental transformation: professional discretion and judgement are being displaced by rigid notions of 'evidence' and 'intelligence' that inform 'risk-assessments' which in turn inform decision-making in an increasing number of areas of our lives. Not only do we tend to view data mining and new technologies as capable of detecting fraud, deception and lies, but also as capable of predicting futures: be they futures of consumption or crime (Ferguson 2017; Mayer-Schönberger & Cukier 2013).

Intelligent surveillance in smart cities promises to 'enhance the safety of citizens by quickly tracing and arresting the imposter' (Rathore et al. 2018: 602). Services such as SocialAuditPro, HypeAuditor or Botometer promise to detect deceptive social bots that impersonate humans, using the same technology and advances in artificial intelligence that enabled them in the first place. But in many cases, 'neither humans nor supervised machine learning algorithms can identify' the fakes (Yang et al. 2019: 50). When trying out the Botometer, created and commercialized by Indiana University, using my Twitter account *@extreme_anthro*, I got to know that the risk of my fiancé being a social bot was whopping 4,2. The results appear hardly trustworthy, the science behind them bogus; upon a closer inspection, false positives dominated among the flagged accounts. But this hardly prevents the product from being sold as a Pro subscription (like the other two, which cannot even be tried out for free) and peddled as scientific, data-driven, AI-powered, and hence free of bias.

'Trust hard data. Not hunches. Trust LineSight®'. This is the tagline of LineSight®, a threat assessment system used by US Customs and Border Patrol and developed by Unisys following the terrorist attacks in 2001. In times of confusion and threats, hard facts and the collection and aggregation of massive amounts of data become particularly seductive, while critical and polemical voices are shut down. After all, who can be against security? But the widespread tendency to view technology, and AI in particular, as neutral, objective (because emotionless), and free of bias is not only deeply problematic but also dangerous. As we know, 'raw data is an oxymoron' (Gitelman 2013). This is not merely a question of correcting bias and ensuring 'transparency', as the neoliberal ideologues and AI ethicists would like to convince us (AI-HLEG 2019). 'Even carefully constructed and transparent algorithms are only as good as the data they process. It is through the data

that algorithms detect patterns and make predictions, and it is the data that determines how well algorithms actually function' (Valentine 2019: 387). But the question is more principal and political: should we at all be governed by algorithms? With one algorithmic risk-assessment, the Botometer robbed my fiancé and many others of their humanity, labelling and profiling them as malicious spam; an opaque decision lacking any accountability. We may not think it so dramatic in this case. But in near future, such risk-assessments can result in widespread closing of accounts deemed *inauthentic*, limiting freedom of speech based on algorithmic decision-making that has an aura of scientific credibility because of the rhetoric of 'data'. Facebook has already been closing down propaganda accounts exhibiting *coordinated inauthentic activity*. But who decides what is inauthentic and what is propaganda? And what does it do to a society to think the world through the lens of the imposter – through the omnipresent possibility that the Other, online or offline, is inauthentic and that inauthenticity as such constitutes a threat? What does it do to us to think the world in these categories?

The same technology is already being used with far more detrimental consequences. AI models and automated decision making with inherent bias is implemented in the digital welfare systems in the UK[4] and US (Eubanks 2018), targeting the poor and already marginalized. These technologies governed by the logic of 'hard data' smoothly integrate with the revival of anthropometry in the form of biometric technologies, such as in *Aadhaar*, the 'biometric welfare system' in India[5], coldly cutting support, food rations, and throwing those in need into ever deeper poverty, and even death – or in the case of facial recognition systems (Gates 2011).

In policing and the criminal justice system across an increasing number of countries, AI-powered software generates false positives and biased risk-assessments that lead to new forms of harm and injustices – be it in the form of predictive policing technologies developed by companies like Palantir or software like the notorious COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) (Kaufmann, Egbert, & Leese 2018; Joh 2017, 2019, 2016). These technologies are designed with two aims: to detect the fraudster-imposter-criminal, and to predict crime and risk. They do so by detecting 'deviance' and abnormal behaviour – capabilities built even into the new generation of intelligent surveillance cameras (Mabrouk & Zagrouba 2017). How this *normal* is determined remains largely opaque, locked in the black box of self-learning algorithms (Riley 2019; Siegel 2013), but it is clear that is not determined by your own actions, but by the actions of others (the reason Botometer thought my fiancé to be a machine is that the pattern of his Twitter activity was perceived by the algorithm as more machine-like based on what it has learned about the typical actions of others; the

---

4 Illuminated by the recent Guardian series 'Automating Poverty' https://www.theguardian.com/technology/series/automating-poverty

5 https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation

fact that the algorithm stands uncorrected and still thinks my fiancé is a machine will only reinforce future bias: now imagine a similar scenario in the criminal justice system). Prejudice and stereotypes smoothly transform into data-driven prediction: if you look like an outlaw biker (or if you are black and poor), you are likely a criminal and future offender. Like the targeted marketing and ads on Facebook based on the analytics of your cookies that track you wherever you roam online, the law will be *in practice* customized through algorithms and adjusted to your individual profile: within this scenario you cannot look like an outlaw biker and expect to be presumed innocent; predictive risk-assessment is not compatible with equality. In the emerging realities of predictive policing and algorithmic governance the statue of Lady Justice has already removed its blindfold and put on Google Glass (or the latest Mojo Lens). These 'weapons of *math* destruction', as O'Neil fittingly called these technologies (O'Neil 2016), do not merely reproduce existing societal and systemic inequities but magnify them in the manner of *self-fulfilling prophecy*, and put them into system, resulting in 'technological redlining' (Benjamin 2019) that either removes or fundamentally alters *human* discretion. Driven by tech-optimism and fears of missing out and falling on diverse rankings measuring levels of digitization, governments are eager to collaborate with the private sector and invest in AI systems for improved, more efficient and *evidence-based* public administration, predictive and *intelligence-led* policing, and military intelligence (Fyfe, Gundhus, & Rønn 2018; Ratcliffe 2016).

This embracement of data-driven algorithmic governance, with its claims to objectivity, value neutrality, efficiency, *intelligence* and *evidence*, is happening under the neoliberal and New Public Management imperatives of *effectivization*, *cutting* personnel *costs* and delivering *measurable* and even more importantly *auditable* results (Shore 2008; Shore & Wright 2015; Hansen, Salskov-Iversen, & Biselev 2002; Strathern 2000). We are not dealing here with a mere technological development, but – *in the current form* (and the technology could be imagined differently) – a material expression of the neoliberal ideology and of the post-political moment. Politics proper is replaced by technocratic audits, assessments, rankings, ethics guidelines, claims to transparency and openness and hopes of ethical self-governance on the part of corporations (Garsten & de Montoya 2008; Garsten & Jacobsson 2011, 2012; Swyngedouw 2018). In the case of Aadhaar, the Indian government not only 'argued that this system would revolutionise welfare: computerised checks would stop fraudsters from siphoning off other people's benefits, allowing more money to reach the poor' (Ratcliffe 2019), but as the former Finance Minister Arun Jaitley put it, it has 'brought transparency and efficiency in governance and helped in transition from cash to less cash economy and informal economy to formal economy.'[6] We should be reminded here that the logic of transparency and audit, as well as the principles of New Public Management, find their origin in Jeremy Bentham's ideas of panoptic surveillance (Bowrey & Smark 2010; Whelan 2013). The neoliberal *logic of transparency* that goes hand in hand with surveillance

[6]https://uidai.gov.in//images/news/Aadhaar_DeMo_GST_are_reforms_that_have_improved_transparency_21112017.pdf

and post-political technocratic governance is fundamentally a *logic of control* and mistrust (Han 2015). Control and exercise of power dressed up as transparency becomes seductive precisely in a state of confusion and disorder, where fakes and imposters appear to proliferate and where people themselves demand and embrace the imposition of checks, controls, and boundaries. And where people impose the very same logic even onto themselves – such as in the quantified self movement and self-tracking (Ajana 2018). The popularity of ever new technologies of social sorting and surveillance in governance is increasing despite the protests against the injustices and harms generated by these systems: be they those of privacy and civil society against LASER (*Los Angeles Strategic Extraction and Restoration*), a racially biased and intrusive predictive policing tool used by LAPD[7] or the anti-Aadhaar nation-wide protests in India in October 2019 that raised not only the issues of injustices and harm caused by the system, but also those of surveillance, profiling, tracking, privacy, and exclusion and biometric governance at large.

Within the neoliberal logic of technocratic governance by transparency and efficiency, trust is replaced by control: nobody can be trusted, everyone can be an imposter, everyone can be corrupt. Digital systems, data mining and advances in machine learning promise a neutral and objective social sorting of the masses of potential imposters and fraudsters. Widespread paranoia is an inevitable consequence of this logic. Technological products that promise to detect and predict deception proliferate. Biometric governance is not only increasingly sophisticated, but also enhanced with deception and lie detectors. Frontex, the European Border and Coast Guard Agency, has been at the forefront of development and testing of new deception detection technologies. One of their experiments involved an 'embodied conversational agent' or ECA, an avatar that conducts an interview with those crossing borders into EU, aimed at detecting signs of deception linked to fraudulent identity documents – changes in voice pitch and ocular movement. They conclude: 'We demonstrated that using both vocalic and ocular measurements we could correctly classify 100% of imposters in a limited scenario while limiting false positives' (Elkins, Derrick, & Gariup 2012: 53), with overall accuracy of 94,47%. The system was based on the contested Interpersonal Deception Theory (IDT) (Buller & Burgoon 1996) and on the controversial theories of the psychologist Paul Ekman that promise to read deception from facial micro expressions (Ekman 1986). These theories have been popularized in 'securitainment' TV shows such as *Lie to Me* (2009 – 2011) (Andrejevic 2010) and became fundamental for the US Transport Security Administration's (TSA) programs in behaviour detection as early as 2002. 'The TSA were willing to ignore forty years' worth of cultural critiques of scientific universalism simply because Ekman's theories promised an efficient means of reading passengers' intentions from the surfaces of their bodies' (Hall 2015: 132). Despite much criticism, theories that promise to deliver

[7] 'LAPD ends another data-driven crime program touted to target violent offenders', Los Angeles Times, 12-04-2019, https://www.latimes.com/local/lanow/la-me-laser-lapd-crime-data-program-20190412-story.html

nothing less than 'the truth' through the 'science of deception', have been influential in border control worldwide and are shaping the developments of intelligent facial recognition systems (Gates 2011). The Paul Ekman Group and other offshot companies have been training law enforcement, border guards, secret services and intelligence agencies for decades in spotting deception through micro expressions and body language. But in the era of artificial intelligence, it is increasingly machines that are being trained based on the same controversial theories, delivering an added sense of 'objectivity', free of the human bias. One such software is iBorderCtrl, tested at the border crossings in Hungary, Greece and Latvia, and developed with 4,5 mil. EUR in support from Horizon 2020, as part of the European Commissions' desire for 'smart borders' to the Cyber-Fortress Europe (Milivojevic 2013). iBorderCtrl integrates biometric data analytics (palm vein, face-matching, fingerprints), document authenticity analytics, 'external legacy and social interfaces' – read: social media accounts analytics, and risk-based assessment systems with a so-called 'automatic deception detection system' that assesses the micro-expressions and so called 'biomarkers of deceit'. This last feature of iBorderCtrl is an artificial intelligence powered 'lie detector', a more advanced version of the Frontex experiment, a virtual policeman avatar that interviews travelers through a pre-arrival screening video and looks for micro expressions that would reveal potential signs of deception and thus *threats*, assigning a risk evaluation to individuals based on how trustworthy they appear in the interview. 'The demand for transparent strangers expresses fear of and hostility toward persons, objects, or situations, that defy immediate understanding and a generalized mistrust of anything unfamiliar or out of the ordinary' (Hall 2015: 134).

In today's world, it is primarily biometric data and the *body surface* that is thought to reveal the impostor; the body itself has become transparent – here again 'the claim that deceivers are transparent, or display universal nonverbal "tells," is based on the research findings of Paul Ekman and his colleagues' (Hall 2015: 138). The same logic of quantification of human behavior is utilized by AI-powered recruiting tools, such as HireVue, used by large companies across the globe to screen potential job applicants through a video interview that is analyzed by artificial intelligence to *predict* their performance, delivering an 'insight score' that ranks all candidates before they even make it to the real interview. All these surveillance, control, risk-based assessment systems and ranking systems, be they employed by governments or private corporations, aim to sort and separate the 'honest' and 'good citizens' from the 'suspect', 'untrustworthy', 'dishonest', 'deviant', and 'criminal' individuals, the 'talented' and 'promising' from the 'useless' that are to be (forever) expelled (as the past of being expelled predicts future expulsions). These automated sorting systems are increasingly pervading all spheres of our lives. Insurance companies, such as the Norwegian *Gjensidige*, are developing risk-based assessment systems to distinguish the 'trustworthy' and 'honest' customers from those who are deemed 'untrustworthy' by what they call a 'smart algorithm built on objective data'. Airbnb has patented an AI-powered trait-analyzing software to screen potential guests – using their social media profiles, news, sites, statements, relations, membership in online groups and other personal digital footprints – in

order to analyze their 'personality' and assign a risk-score (i.e. the likelihood of you trashing a rented apartment); 'traits such as "neuroticism and involvement in crimes" and "narcissism, Machiavellianism, or psychopathy" are "perceived as untrustworthy"' (Blunden 2020). How these algorithms work, on which data they base these judgements, remains unknown. On the Airbnb website we can read:

> Every Airbnb reservation is scored for risk before it's confirmed. We use predictive analytics and machine learning to instantly evaluate hundreds of signals that help us flag and investigate suspicious activity before it happens.[8]

Airbnb uses the same technology and logic as the one driving predictive policing and risk-assessments within the criminal justice system to sort individuals and weed out potential deviants of all kinds (Joh 2016). Services such as *Autohost* already offer 'guest screening' for hospitality, integrating ID verification with criminal background checks (even if you have 'done your time' and justice has been served, you are to continue to be punished, judged and sentenced time and again – loan, insurance, hotel stay – shall be beyond your reach), their system utilizing artificial intelligence and machine learning is:

> Built on top of our risk assessment engine, each guest goes through a dynamic set of screens that collect different types of information based on the guest's risk level. Our fraud model identifies the guest using a digital footprint to make sure the guest is unique in our ecosystem. The guest is asked to provide personal information that is validated against worldwide databases. …We check the guest against all social media platforms *to make sure they're real* and have a presence, letting your team know if we flag anything abnormal (emphasis by author).[9]

Wherever we turn, the same logic of risk, threat, and mistrust is present; anyone can be an impostor, a fake, *unreal*. Workplace surveillance technologies and automated worker profiling software are another booming market predicated upon the same logic (Ball 2010). They promise to increase productivity, efficiency, unlock the full potential of individuals and organizations, ensure compliance and transparency while monitoring and analyzing anything from staff calendars, to their mood and facial expressions, toilet breaks, keyboard activity, location through wearable tech, or social media use outside of working hours. All this data can be easily misused by employers, increase pressure on workers, and spread a culture of fear, control, paranoia and mistrust. There is little doubt that 'automated data processing exponentially increases the chances of workers' rights being

---

8 https://www.airbnb.com/help/article/2356/what-does-it-mean-when-someones-id-has-been-checked (accessed 19 January 2020).

9 https://www.autohost.ai/features/ (accessed 19 January 2020).

violated' (Todolí-Signes 2019: 470). While practices of social sorting are not new, what is new is the degree to which they have become automated, exploited by those with disproportionate power, be they corporations or governments, and dressed in the rhetoric of objectivity, neutrality and transparency. The private security industry is booming, not necessarily because it tackles real threats and risks, but because it has become an expert in 'the construction and production of *ontological security* through three mechanisms: risk identification, risk profiling and risk management' (Krahmann 2018: 357, emphasis mine), which coincide with the modes of the currently hegemonic technocratic governance. And what is even more startling, is the rapid normalization and embracement of these technologies.

Authenticity, Authentication and Authorization

The widespread sense of confusion, chaos, disorder and generalized mistrust thus not only creates an obsession with social sorting and profiling, but also a preoccupation with *authenticity*, truth, and identity – the flip side of the obsession with security, borders, protection, and control. In a world populated by fakes, marketing, spin-doctoring, propaganda and fraud, consumers – as much as governments checking borders and corporations hiring employees – are in search of authenticity; *authenticity sells* (Gilmore & Pine 2007). Authenticity itself becomes pre-packaged and commodified, a hoax (Potter 2010), and yet, our desire for it only increases, paradoxically generating ever new sources of inauthenticity, and demand for products and solutions that sort the authentic from the inauthentic. Even the acts of modern terrorists can no longer be explained by recourse to religious dogma but are 'better understood as an expression of the modern quest for subjectivity and authenticity' (Verkaaik 2004: 45). In a disenchanted world, as Lindholm put it, the

> quest for the authentic grounding becomes increasingly pressing as certainty is eroded and the boundaries of the real lose their taken-for-granted validity (…) The search for a sense of authenticity is the most salient and pervasive consequence of the threats modernity makes to our ordinary reality and sense of significance. (…) Like medieval monks, we all now must look for something sacred to hold on to, but without the possibility of gaining any exterior authentication; there is no certification of the really real anymore, and anything can be a forgery. (…) The sacred is where you find it (Lindholm 2002: 337).

The more we feel the loss of these boundaries between the real and the fake, truth and lie, the more we appear to crave them. Within the current neoliberal order, it means that authenticity is simultaneously *commodified* and *securitized* – while security is commodified, and consumption securitized. Paranoia emerges from within this double movement. Certificates and proofs of authenticity and origin are proliferating, as do organizations that authenticate, verify, and rank, resulting in organizational change and standardization of institutions in the image of the performance

indicators that are being raked (Sauder & Espeland 2009). The idea of authenticity is packaged into anything from Coca Cola, 'the real thing,' to the 'authentic leader development' courses at the Harvard Business School. Even parkour and other forms of 'edgework' and countercultural rebellion with an aura of authenticity have not escaped commodification (Raymen 2019; Frank 1998; Heath & Potter 2005). The realm of security has become infused with the same vision of authenticity, security itself collapsing into practices and technologies of verification and authentications, i.e. detection of imposters. The politics of citizenship, to use an example, has been transformed into identity management that, with the help of biometric and deception detection technologies 'introduces an obsession with authentication' (Muller 2009: 88). As Muller argues,

> identity management seemingly circumvents the complications associated with identifying the enemy and the friend, and simply makes the discrimination between the authentic and the inauthentic. No longer capable of knowing/identifying the enemy, identity management shifts its focus to authentication and authorization. Relying on complex algorithms and electronic referencing through databanks, biometrics is capable of verifying and discriminating between the qualified and the unqualified bodies, as the politics of (inclusion) exclusion sees itself moving beyond the imprecision of racial profiling and towards the technologically advanced sanitary discriminations of identity management. (…) The rising obsession with so-called 'identity theft' or 'identity fraud' is an important link in the securitization of citizenship and the shift towards 'identity management' (Muller 2009: 84-5).

At the heart of this type of social sorting and profiling is precisely the obsession with separating – in a surgical and sanitized manner – the authentic from the inauthentic, the pure from the impure: the 'real thing' from the imposter. Social sorting by authentication in turn authorizes the *authenticated* individual to receive anything from rights to food rations – and makes the individual trustworthy.

While we often imagine subcultures as outside or at the periphery of society, as those who are deviant, neither fully integrated nor abiding by societal norms, this perception is grounded in an aesthetic deception, in our prejudice based on appearances. Elsewhere, we have argued that the opposite is often the case (Kuldova 2018b; Sánchez-Jankowski 2018). That is, criminal subcultures, to return to the outlaw motorcycle clubs, often reveal existing societal tendencies and the cultural logic that permeates our societies in an *extreme* or exaggerated form. It is precisely in this sense that they are good to think.

If there is one thing that attracts people to outlaw motorcycle clubs, it is the promise of authenticity; of becoming a *real* and *authentic* biker. Not a hobby rider that dresses up for the weekend in Harley Davidson gear, a so-called wannabe, but the

real deal, an *authentic* and *ritually authenticated* member of the outlaw motorcycle subculture that has gone through the process of selection and authentication and made it into the ranks of the selected few. And if there is one thing that the clubs fear the most, it is the imposter: be it a wannabe or an undercover agent. Both are perceived as a *dangerous threat* and represent a risk of *pollution* of the *pure*, authentic brotherhood (Douglas 2002). Like Coca-Cola, outlaw motorcycle clubs promise their members 'the real thing'; in a world populated by fakes and wannabes, they market themselves as the bearers of authenticity. The patch, the club logo, is not only a brand but *a mark of authenticity* and of origin, and as such a mark of belonging produced and bestowed by the club onto newly patched-in members following a long period of trials, background checks, trustworthiness and risk-assessments, and identity verification. Unlike an ordinary brand, its aura of authenticity resides in the simple fact that the patch cannot be bought, it has to be earned. As such, it is *inalienable* (Weiner 1992). In a world of commodities, of deception and fake promises, the outlaw motorcycle clubs offer something real reserved to carefully selected and screened members; this is what attracts many to the subculture. This inalienable patch is considered *sacred* by the members; no insults of the patch are tolerated and the patch design is legally protected, counterfeiters receive cease and desist letters and are brought to the court of law, and those sporting counterfeits on the street are dealt with using violence and threats (Kuldova 2019d, 2017a, 2018d). Hells Angels patented their notorious 'death head' already in 1972 and trademarked it in 1978 in the US and later in Europe, other transnational outlaw motorcycle clubs followed. 'Authenticity' must be protected from imposters and those challenging its authority and its power: be it by (the threat of) violence or the law (paradoxically instrumentalized by the self-declared outlaws). Identity, another dominant contemporary preoccupation, depends on it.

The global expansion of the outlaw motorcycle clubs depends on the maintenance and policing of the boundary between the pure and the impure, the authentic and the inauthentic, the real and the fake – by violent and legal means. This is the essence of their business model and their growth. But the content of this authenticity has been transformed since the emergence of the subculture in California after the Second World War: (1) the wild and rebellious counterculture has been progressively *commodified* both by external actors and the bikers themselves in the quest to expand their territories and attract new members – the clubs have become recognizable *brands*, trademarked their logos and registered themselves as companies; (2) this has led to the professionalization and bureaucratization of the subculture as it has transnationally expanded; and to a consequent (3) transformation of authenticity into *authentication* and *authorization* at the same time as the 'patches' of the clubs, sacred to the members, have been turned into fetishized brands (Kuldova 2017a, 2019a). This *securitization of authenticity* has not only been a result of organizational change within the context of consumer society but has been driven by the paranoia of the imposter and by the desire to secure the remains of the authentic and *sacred* core, of that which is inalienable and beyond commodification, available only to the authenticated members. Securitization of authenticity is thus also a matter of 'securitization of the spiritual-moral values' of the subculture (Østbø

2017), the very values that make it seductive to their supporters, to people often disoriented, lacking direction, expelled by neoliberal markets and seeking recognition. In the patch, they are recognized as officially belonging to a powerful transnational brotherhood, which also guarantees their symbolic immortality (Kuldova 2019b).

The patch can be understood as a stamp of authenticity, a mode of certification, a proof of belonging and a proof that one can legitimately claim the criminal capital and power mystique of the club – both a right and entitlement. As an authorized member, one has certain privileges (much like in an elitist luxury club of selected few). But one also has duties that must be performed on behalf of the club, they may include self-sacrifice on behalf of the club. It is in this sense that the 'border-control' performed by the clubs mirrors the one performed by the state. The authentication and consequent authorization processes rely increasingly on 'data-collection' and 'intelligence'. Prospects have to produce – over time – evidence that they will be an asset to the club; the burden of proof is on them. The overall performance and collected data are in turn evaluated by the club members, who not only intensely observe and analyze the behavior of the prospects in different situations, but also check their credentials, often through intrusive methods – not shying away from placing bugs in cars or homes. These methods are deemed necessary to protect the brotherhood from imposters – undercover agents or wannabes – individuals that inflate their power, capabilities, skills and their self at large. Boundaries must be protected, only those carefully vetted are allowed in – to enjoy the benefits of the collective. It is also in this sense that the clubs act as sovereigns – not only do they decide over life and death (or at least cultivate a reputation for doing so) – but they make sovereign decisions about membership and expulsion; a god-like power that has been associated with the state (Shammas 2018). And indeed, in many respects the gangs act like states – after all, they are in the same business, namely *protection*.

Attempts at infiltrating the clubs by undercover police and exposure to new surveillance technologies have made the clubs not only paranoid and suspicious of anyone attempting to come close but have also turned them into self-styled experts on deception detection. Not unlike the police are trained to detect deception, be it through training in body language or with the help of AI-powered software, the clubs develop their own techniques of deception detection: of behavioral tests and trials, of profiling, stereotyping, and verification; a combination of soft skills and intimidation. Trust as a default attitude in a social encounter is replaced by a paranoid search for signs of deception and impostering. A case in point: aware of the proliferating online fake social media accounts run by law enforcement, outlaw bikers create closed groups on Facebook that require elaborate verification through personal acquaintance and goodwill of a minimum of five already authenticated members (who are in turn willing to take the personal risk of vouching on behalf of a given person). Online channels where profiles suspect of belonging to members of law enforcement are posted and consequently investigated are proliferating. These practices could be understood as counterintelligence. New tech-

nologies that track online activities and flag suspicious behavior of selected users are deployed on club fora with limited access – fora which happen to be of great interest to law enforcement and intelligence agencies. Hackers are increasingly finding their place within the clubs, providing similar services to those offered to police forces by private tech companies (even I have been screened in this manner by one of the clubs, which managed to produce several hundred pages on my person). The tech race is on – on both sides. This everyday exposure to both low-tech and high-tech surveillance, where police drones become a common sight at parties organized by the club, has turned many within these clubs into experts on security. Clubhouses of some of the largest international OMCs are often equipped with app-integrated intelligent surveillance cameras that notify members of any suspicious activity, lists of 'suspects' is generated based on 'intelligence' collected, and members and prospects are to be 'resilient' during open club events, monitoring 'the situation'. This understanding of surveillance, security, privacy and *interest* is something that many of the club members effectively monetize through the legal private security companies that they run (as some would claim, partly to launder illegal proceeds). Active in the night-time economy and private security, delivering bouncers, private security guards and personal bodyguards, as well as mobilizing vigilante groups, the clubs are often engaged in alternative forms of 'community policing' as they struggle to gain legitimacy and monopoly on violence in their area, while blaming the police for failing the community and failing to provide security. Police are increasingly seen as a competing gang in town, utilizing the same logic. An environment of mistrust, where competing actors attempt to take control, emerges; both actors are in the business of determining who is fake and who is real, who is an imposter and therefore a threat. The bouncer is not unlike a risk-assessment algorithm – more humane and less informed, indeed, but often equally prejudiced. At this point we should ask ourselves if soon our own neighborhoods, communities and even families will not transform themselves into securitized units along this model. The proliferation of vigilante groups in conjunction with neighborhood surveillance smart tech, such as Amazon's Ring, indeed points into the same direction. Are we far too willing to perceive the Other as an imposter, and a threat – by default?

Paranoid Cultures: What If They Are Really After You?

The degree to which new intelligent surveillance technologies create an environment of paranoia can indeed be disputed. We can also ask ourselves if we are dealing with a culture of paranoia at all when undercover agents really are after you (Lee 2017), or when your 'digital footprint' is used to create your psychological profile that may prevent you from booking a hotel room. If you take both seriously – we could claim that you are at once justified in your paranoia, but nonetheless still paranoid. I leave this judgement to the reader. But while many of us are still willingly and indiscriminately sharing some of the most private information online, living under the motto that if you do no wrong you have nothing to hide (a motto that defies the logic of privacy), others experiencing the effects, harms and injustices of surveillance first-hand, on their bodies, may think otherwise. As with-

in the outlaw motorcycle clubs, a culture of paranoia may become dominant in society at large: a culture where trust, rights, access, depends on vetting, authentication and background checks – a culture where, simultaneously, these checks are never enough as more data can always be gathered, evaluated and result in a new risk-assessment score; suspicion persists *despite* all possible authentications and certificates – or maybe, precisely *because* of them. A culture where nothing you say can be taken at face value, where doubt lurks behind every encounter – at the very same time as you make trust your selling point (not unlike most contemporary governments). Stivers offers a compelling definition of paranoia, that resonated both with our observations of the outlaw motorcycle subculture and with cultural tendencies at large,

> most widespread characteristics of paranoia are suspiciousness and guardedness. The paranoid person is constantly preparing to deal with variegated threats, including insults, snubs, sarcasm, criticism, commands, or even physical threats. (…) Paranoid people exhibit suspicious thinking that is above all rigid. They cannot be persuaded that their suspicions are unfounded, and they are highly selective in the way they marshal facts, perceptions, and innuendoes. In making the unshakable assumption that others pose a threat to them, paranoid people scrutinize every word and facial expression for signs of hostility, rejection, and even indifference. Like religious fanatics, they hold their perceptions and interpretations to be infallible. The paranoid are thus closeminded. Their inability to accept uncertainty and ambiguity further indicates paranoid rigidity: Better to anticipate the worst than to be surprised in a state of naive optimism. (…) Paranoid suspicion is a perfect example of self-fulfilling prophecy (….) Someone who wishes to protect himself against potentially dangerous people must be continuously suspicious of them. In a situation of near complete ambiguity, suspicion is the best way to maintain security. (…) Paranoia emanates from an intense threat to autonomy. Paranoid people live in a continuous state of vigilance and are ready for any surprise or emergency (Stivers 2004: 125-6).

While we can easily see all the elements of paranoia mentioned by Stivers coming to life in the actions of the bikers as much as of law enforcement, states and private corporations, we should pay particular attention to the following: *paranoia emanates from an intense threat to autonomy*. It is precisely autonomy that we risk losing in an age of intelligent surveillance. It is a revealing paradox that 'greedy institutions' such as outlaw motorcycle clubs lure in new members precisely through their promise of autonomy and sovereignty. But even there, as elsewhere, autonomy has become just a newspeak for control. Much like authenticity, autonomy and sovereignty become an impossibility within the current order.

Coda

When parents cannot resist the temptations of apps such as PanSpy: the 'ultimate parental control solution', and play Big Brother with their own family, tracking the whereabouts of their children, their cell phone activity, view complete record of all communication, monitor app use, and remotely control apps, it is no wonder that governments fall into the same trap. Or as PanSpy puts it: 'after all, you don't want them exchanging SMS with any wrong sorts of people or hiding dubious boyfriends, do you?'[10] When surveillance within the family is becoming the new norm, sold through the very same images of external threats as predictive policing and military tech, and with the promise of keeping children safe and rid the parent of doubts, will there even be critical voices in the future? When we normalize the hardline distinction between the 'good' and 'those to be feared', determined by what we are told are 'objective' algorithms, will there be any scope for critical thinking left, any scope for doubt, and ultimately for justice? When we are so keen to replace trust with control in our own homes and eliminate any possibility of our own children's privacy, when we are so keen to rob them of their moral right to privacy (Montague 1988) in exchange for a sense of power, can we expect the government to act any differently? The seductions of power are great, and the visions of power promised by artificial intelligence surveillance systems are particularly grand: total control over populations, objective determination of threats, and prediction of the future itself – nothing less than visions of omniscience and omnipotence. Many of those promises are bogus, predictions based on historical data are little more than often bad statistics put into system, 'dirty data' lead not only to wrong conclusions but to injustices and new forms of 'algorithmic harm', and the great amount of false positives generated by these systems makes them hardly reliable. But in the quest for power, for order, for control, we are led to ignore this knowledge and sacrifice critical reason itself. Do we risk becoming like paranoid criminal organizations – even if we have nothing, unlike them, to hide? Do we risk fighting for civil rights – like them – while submitting ourselves and our closest to the same logic of oppressive surveillance that we criticize? Do we risk treating the Other as always already a potential imposter?

Author Bio

Tereza Østbø Kuldova is a social anthropologist and senior researcher based at the Work Research Institute, Oslo Metropolitan University. She is the author of, among others, *How Outlaws Win Friends and Influence People* (Palgrave, 2019), *Luxury Indian Fashion: A Social Critique* (Bloomsbury, 2016), editor of *Crime, Harm and Consumerism* (Routledge, 2020), *Outlaw Motorcycle Clubs and Street Gangs: Scheming Legality, Resisting Criminalization* (Palgrave, 2018), *Urban Utopias: Excess and Expulsion in Neolib-*

[10] https://www.panspy.com/sent-received-sms.html (accessed December 13, 2019).

eral South Asia (Palgrave, 2017), and *Fashion India: Spectacular Capitalism* (Akademika Publishing, 2013). She has written extensively on topics ranging from fashion, design, aesthetics, branding, intellectual property rights, nationalism, philanthropy, India, to outlaw motorcycle clubs, subcultures, and organized crime. She is the founder and editor-in-chief of the *Journal of Extreme Anthropology* and of the *Extreme Anthropology Research Network;* in 2020 she has founded the *Algorithmic Governance: Research Network*. For more information, please visit: www.tereza-kuldova.com.

References

AI-HLEG. 2019. Ethics Guidelines for Trustworthy AI: High-Level Expert Group on Artificial Intelligence. European Commission (Brussels). https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Ajana, B., ed. 2018. Self-Tracking: Empirical and Philosophical Investigations. Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-65379-2

Altheide, D. L. 2006. 'Terrorism and the Politics of Fear.' Cultural Studies 6 (4): 415-439. https://doi.org/10.1177/1532708605285733

Althusser, L. 1971. 'Ideology and Ideological State Apparatuses' In Lenin and Philosophy, and Other Essays edited by trans. Ben Brewster, 127-188. London: New Left Books.

Andrejevic, M. 2010. 'Reading the Surface: Body Language and Surveillance.' Culture Unbound: Journal of Current Cultural Research 2: 15-36. https://doi.org/10.3384/cu.2000.1525.102315

Ball, K. 2010. 'Workplace Surveillance: An Overview.' Labor History 51 (1): 87-106. https://doi.org/10.1080/00236561003654776

Bataille, G. 1993. The Accursed Share: Volumes II and III. New York: Zone Books.

Bauman, Z., and D. Lyon. 2013. Liquid surveillance: a conversation. Cambridge: Polity.

Beck, U. 1992. Risk Society: Towards a New Modernity. London: Sage.

Benedek, L. 1953. The Wild One. United States: Columbia Pictures.

Benjamin, R. 2019. Race After Technology: Abolitionist Tools for the New Jim Code. Medford, MA: Polity Press. https://doi.org/10.1093/sf/soz162

Blunden, M. 2020. 'Booker beware: Airbnb can scan your online life to see if you're a suitable guest.' Evening Standard, 3 January 2020, 2020. https://www.standard.co.uk/tech/airbnb-software-scan-online-life-suitable-guest-a4325551.html

Bowrey, G. D., and C. J. Smark. 2010. 'The influence of Jeremy Bentham on recent public sector financial reforms.' Journal of New Business Ideas and Trends 8 (1): 1-10.

Breton, H. O. 'Coping with a Crisis of Meaning: Televised Paranoia.' In Media and the Inner World: Psycho-cultural Approaches to Emotion, Media and Popular Culture, edited by Caroline Brainbridge and Candida Yates, 113-134. New York: Palgrave Macmillan. https://doi.org/10.1057/9781137345547_8

Buller, D. B., and J. K. Burgoon. 1996. 'Interpersonal Deception Theory.' Communication Theory 6: 203-242. https://doi.org/10.1111/j.1468-2885.1996.tb00127.x

Campbell-Verduyn, M., M. Goguen, and T. Porter. 2017. 'Big Data and algorithmic governance: the case of financial practices.' New Political Economy 22 (2): 219-236. https://doi.org/10.1080/13563467.2016.1216533

Coser, L. A. 1974. Greedy Institutions: Patterns of Undivided Commitment. New York: The Free Press.

Dobyns, J. 2010. No Angel: My Undercover Journey to the Dark Heart of Hells Angels. Chatham: Canongate Books.

Douglas, M. 2002. Purity and Danger: An Analysis of Concepts of Pollution and Taboo. London: Routledge. https://doi.org/10.4324/9780203361832

Ekman, P. 1986. Telling lies: clues to deceit in the marketplace, politics, and marriage. New York: Berkley.

Elkins, A. C., D. C. Derrick, and M. Gariup. 2012. 'The Voice and Eye Gaze Behavior of an Imposter: Automated Interviewing and Detection for Rapid Screening at the Border.' Proceedings of the EACL 2012 Workshop on Computational Approaches to Deception Detection: 49-54.

Eubanks, V. 2018. Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. St. Martin's Publishing Group.

Ferguson, A. G. 2017. The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement. New York: New York University Press. https://doi.org/10.2307/j.ctt1pwtb27

Frank, T. 1998. The Conquest of Cool: Business, Culture, Counterculture, and the Rise of Hip Consumerism. Chicago: University of Chicago Press. https://doi.org/10.7208/chicago/9780226924632.001.0001

Frosh, S. 2016. 'Relationality in a Time of Surveillance: Narcissism, Melancholia, Paranoia.' Subjectivity 9 (1): 1-16. https://doi.org/10.1057/sub.2015.19

Furedi, F. 2002. Culture of Fear. London: Continuum International.

Fyfe, N., H. Gundhus, and K. V. Rønn, eds. 2018. Moral Issues in Intelligence-led Policing. London: Routledge. https://doi.org/10.4324/9781315231259

Garsten, C., and M. L. de Montoya, eds. 2008. Transparency in a New Global Order: Unveiling Organizational Visions. Cheltenham: Edward Elgar. https://doi.org/10.4337/9781848441354

Garsten, C., and K. Jacobsson. 2011. 'Transparency and legibility in international institutions: the UN Global Compact and post-political global ethics.' Social Anthropology 19 (4): 378-393. https://doi.org/10.1111/j.1469-8676.2011.00171.x

Garsten, C., and K. Jacobsson. 2012. 'Post-Political Regulation: Soft Power and Post-Political Visions in Global Governance.' Critical Sociology 39 (3): 421-437. https://doi.org/10.1177/0896920511413942

Gates, K. A. 2011. Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. New York: New York University Press. https://doi.org/10.18574/nyu/9780814732090.001.0001

Gilmore, J. H., and J. B. Pine. 2007. Authenticity: What Consumers Really Want. Harvard: Harvard Business Press.

Giroux, H. A. 2015. 'Totalitarian Paranoia in the Post-Orwellian Surveillance State.' Cultural Studies 29 (2): 108-140. https://doi.org/10.1080/09502386.2014.917118

Gitelman, L., ed. 2013. "Raw Data" Is an Oxymoron. Cambridge, Massachusetts: MIT Press.
https://doi.org/10.7551/mitpress/9302.001.0001

Hall, R. 2015. The Transparent Traveller: The Performance and Culture of Airport Security. Durham: Duke University Press.
https://doi.org/10.1215/9780822375296

Hallsworth, S., and J. Lea. 2011. 'Reconstructing Leviathan: Emerging Contours of the Security State.' Theoretical Criminology 15 (2): 141-157.
https://doi.org/10.1177/1362480610383451

Han, B.-C. 2015. The Transparency Society. Stanford: Stanford University Press.

Hansen, H. K., D. Salskov-Iversen, and S. Biselev. 2002. 'Discursive globalization: transnational discourse communities and New Public Management.' In Towards a Global Polity, edited by M. Ougaard and R. Higgott, 107-124. London: Routledge.

Harper, D. 2008. 'The Politics of Paranoia: Paranoid Positioning and Conspiratorial Narratives in the Surveillance Society.' Surveillance & Society 5 (1): 1-32.
https://doi.org/10.24908/ss.v5i1.3437

Heath, J., and A. Potter. 2005. The Rebel Sell: How the counterculture became consumer culture. West Sussex: Capstone Publishing.

Holm, N. 2009. 'Conspiracy Theorizing Surveillance: Considering Modalities of Paranoia and Conspiracy in Surveillance Studies.' Surveillance & Society 7 (1): 36-48.
https://doi.org/10.24908/ss.v7i1.3306

Jameson, F. 1988. 'Cognitive Mapping.' In Marxism and the Interpretation of Culture, edited by C. Nelson and L. Grossberg, 347-360. Urbana: University of Illinois Press.
https://doi.org/10.1007/978-1-349-19059-1_25

Joh, E. E. 2016. 'The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing.' Harvard Law & Policy Review 10: 15-43.

Joh, E. E. 2017. 'Artificial Intelligence and Policing: First Questions.' Seattle University Law Review 41: 1139-1144.

Joh, E. E. 2019. 'The Consequences of Automating and Deskilling the Police.' UCLA Law Review Discourse: 1-34.

Katzenbach, C., and L. Ulbricht. 2019. 'Algorithmic Governance.' Internet Policy Review 8 (4): 1-18.

Kaufmann, M., S. Egbert, and M. Leese. 2018. 'Predictive Policing and the Politics of Patters.' The British Journal of Criminology: 1-19. https://doi.org/10.1093/bjc/azy060

Krahmann, E. 2018. 'The Market for Ontological Security.' European Security 27 (3): 356-373. https://doi.org/10.1080/09662839.2018.1497983

Kuldova, T. 2017a. 'Hells Angels Motorcycle Corporation in Fashion Business: On the Fetishism of the Trademark Law.' Journal of Design History 30 (4): 389-407. https://doi.org/10.1093/jdh/epw041

Kuldova, T. 2017b. 'The Sublime Splendour of Intimidation: On the Outlaw Biker Aesthetics of Power.' Visual Anthropology 30 (5): 379-402. https://doi.org/10.1080/08949468.2017.1371545

Kuldova, T. 2018a. 'The "Ethical Sell" in the Indian Luxury Fashion Business.' In European fashion: The creation of a global industry, edited by Veronique Pouillard and Regina Blaczczyk, 263-282. Manchester: Manchester University Press.

Kuldova, T. 2018b. 'Introduction: Scheming Legality, Resisting Criminalization.' In Outlaw Motorcycle Clubs and Street Gangs: Scheming Legality, Resisting Criminalization, edited by Tereza Kuldova and Martín Sánchez-Jankowski. New York: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-76120-6

Kuldova, T. 2018c. 'Outlaw Bikers Between Identity Politics and Civil Rights.' In Outlaw Motorcycle Clubs and Street Gangs: Scheming Legality, Resisting Criminalization, edited by Tereza Kuldova and Martin Sanchez-Jankowski, 175-203. New York: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-76120-6_8

Kuldova, T. 2018d. 'Protecting Trademarks and 'Culture': Outlaw Motorcycle Clubs in Between Counterculture and Popular Culture.' In Outlaw Motorcycle Clubs and Street Gangs: Scheming Legality, Resisting Criminalization, edited by Tereza Kuldova and Martin Sanchez-Jankowski. New York: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-76120-6

Kuldova, T. 2018e. 'When elites and outlaws do philanthropy: on the limits of private vices for public benefit.' Trends in Organized Crime 21 (3): 295-309. https://doi.org/10.1007/s12117-017-9323-6

Kuldova, T. 2019a. 'Fetishism and the Problem of Disavowal.' Qualitative Market Research 22 (5): 766-780.
https://doi.org/10.1108/QMR-12-2016-0125

Kuldova, T. 2019b. How Outlaws Win Friends and Influence People. New York: Palgrave Macmillan.
https://doi.org/10.1007/978-3-030-15206-2

Kuldova, T. 2019c. 'Popular Culture, Populism and the Figure of the "Criminal": On the Rising Popular Support of Outlaw Bikers and Anti-establishment Resentment.' In Crime, Deviance and Pop Culture, edited by A. Antoniou and D. Akrivos. New York: Palgrave Macmillan.
https://doi.org/10.1007/978-3-030-04912-6_10

Kuldova, T. 2019d. 'Re-thinking Solidarity at the Fringes of Consumer Culture: What do Outlaw Bikers Have that "Brand Communities" Lack?' Journal of Culture 8 (1): 2-12.

Kuldova, T. 2020. 'Luxury Brands in the Wrong Hands: Of Harleys, Harm, and Sovereignty.' In Crime, Harm and Consumerism, edited by Steve Hall, Tereza Kuldova and Mark Horsley. London: Routledge.
https://doi.org/10.4324/9780429424472-8

Kuldova, T., and J. Quinn. 2018. 'Outlaw Motorcycle Clubs and Struggles over Legitimization.' In Outlaw Motorcycle Clubs and Street Gangs: Scheming Legality, Resisting Criminalization, edited by Tereza Kuldova and Martin Sanchez-Jankowski, 145-173. New York: Palgrave Macmillan.
https://doi.org/10.1007/978-3-319-76120-6_7

Kuldova, T., and M. Sánchez-Jankowski. 2018. Outlaw Motorcycle Clubs and Street Gangs: Scheming Legality, Resisting Criminalization. New York: Palgrave Macmillan.
https://doi.org/10.1007/978-3-319-76120-6

Lee, B. J. 2017. '"It's not paranoia when they are really out to get you': the role of conspiracy theories in the context of heightened security.' Behavioral Sciences of Terrorism and Political Aggression 9 (1): 4-20.
https://doi.org/10.1080/19434472.2016.1236143

Lindenmuth, K. 2019. 'Prevention or Self-Fulfilling Prophecy? Predictive Policing's Erosion of the Presumption of Innocence.' Law School Student Scholarship. 1018: 1-29.

Lindholm, C. 2002. 'Authenticity, Anthropology, and the Sacred.' Anthropological Quarterly 75 (2): 331-338.
https://doi.org/10.1353/anq.2002.0035

Linke, U., and D. T. Smith. 2009. Cultures of Fear: A Critical Reader. London: Pluto Press.

Lyotard, J.-F. 1984. The Postmodern Condition: A Report on Knowledge. Manchester: Manchester University Press.
https://doi.org/10.2307/1772278

Mabrouk, A. B., and E. Zagrouba. 2017. 'Abnormal Behavior Recognition for Intelligent Video Surveillance Systems: A Review.' Expert Systems with Applications 91: 480-491.
https://doi.org/10.1016/j.eswa.2017.09.029

Mayer-Schönberger, V., and K. Cukier. 2013. Big Data: A Revolution that Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt.

Mbadiwe, T. 2018. 'Algorithmic Injustice.' The New Atlantis: A Journal of Technology & Society Winter: 3-28.

Milivojevic, S. 2013. 'Borders, technology and (im)mobility: "Cyber- Fortress Europe" and its emerging Southeast frontier.' Australian Journal of Human Rights 19 (3): 101-123.
https://doi.org/10.1080/1323-238X.2013.11882136

Montague, P. 1988. 'A Child's Right to Privacy.' Public Affairs Quarterly 2 (1): 17-32.

Morgan, G., S. Dagistanli, and G. Martin. 2010. 'Global Fears, Local Anxiety: Policing, Counterterrorism and Moral Panic Over "Bikie Gang Wars" in New South Wales.' The Australian and New Zealand Journal of Criminology 43 (3): 580-599.
https://doi.org/10.1375/acri.43.3.580

Muller, B. F. 2009. '(Dis)qualified bodies: Securitization, Citizenship and "identity management".' In Securitizations of Citizenship, edited by P. Nyers, 77-93. London: Routledge.

O'Neil, C. 2016. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York: Crown.

Østbø, J. 2017. 'Securitizing "spiritual-moral values" in Russia.' Post-Soviet Affairs 33 (3): 200-216.
https://doi.org/10.1080/1060586X.2016.1251023

Potter, A. 2010. The Authenticity Hoax: How We Get Lost Finding Ourselves. London: Scribe Publications.

Power, M. 2004. The Risk Management of Everything: Rethinking the Politics of Uncertainty. London: DEMOS.

Queen, W. 2011. Under and Alone: The True Story of the Undercover Agent Who Infiltrated America's Most Violent Outlaw Motorcycle Gang. Edinburgh: Mainstream Publishing.

Ratcliffe, J. H. 2016. Intelligence-Led Policing. London: Routledge. https://doi.org/10.4324/9781315717579

Ratcliffe, R. 2019. 'How a glitch in India's biometric welfare system can be lethal.' The Guardian, 16 October 2019, 2019. https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation.

Rathore, M. M., A. Paul, W.-H. Hong, H. Seo, I. Awan, and S. Saeed. 2018. 'Exploiting IoT and big data analytics: Defining Smart Digital City using real-time urban data.' Sustainable Cities and Society 40: 600-610. https://doi.org/10.1016/j.scs.2017.12.022

Raymen, T. 2019. Parkour, Deviance and Leisure in the Late Capitalist City. Bingley: Emerald Publishing. https://doi.org/10.1108/9781787438118

Riley, P. 2019. 'Three Pitfalls in Machine Learning.' Nature 572: 27-29. https://doi.org/10.1038/d41586-019-02307-y

Rothstein, H., M. Huber, and G. Gaskell. 2006. 'A theory of risk colonization: the spiralling regulatory logics of societal and institutional risk.' Economy and Society 35 (1): 91-112. https://doi.org/10.1080/03085140500465865

Sánchez-Jankowski, M. 2018. 'Gangs, Culture and Society in United States.' In Outlaw Motorcycle Clubs and Street Gangs: Scheming Legality, Resisting Criminalization, edited by Tereza Kuldova and Mártin Sánchez-Jankowski. New York: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-76120-6_2

Sandberg, S., and V. L. Shammas. 2015. 'Habitus, capital, and conflict: Bringing Bourdieusian field theory to criminology.' Criminology & Criminal Justice: 1-19. https://doi.org/10.1177/1748895815603774

Sauder, M., and W. N. Espeland. 2009. 'The Discipline of Rankings: Tight Coupling and Organizational Change.' American Sociological Review 74: 63-82.
https://doi.org/10.1177/000312240907400104

Schmitt, C. 2007. The Concept of the Political. Chicago: University of Chicago Press.

Shammas, V. L. 2018. 'The State as God: On Bourdieu's Political Theology.' Journal of Extreme Anthropology 2 (2): 61-77.
https://doi.org/10.5617/jea.6601

Shore, C. 2008. 'Audit culture and lliberal governance: Universities and the politics of accountability.' Anthropological Theory 8 (3): 278-298.
https://doi.org/10.1177/1463499608093815

Shore, C., and S. Wright. 2015. 'Audit Culture Revisited: Rankings, Ratings, and the Reassembling of Society.' Current Anthropology 56 (3): 421-444.
https://doi.org/10.1086/681534

Siegel, E. 2013. Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die. Hoboken, New Jersey: John Wiley & Sons, Inc.

Silverman, S. J. 2016. '"Imposter Children" in the UK Refugee Status Determination Process.' Refuge 32 (3): 30-39.

Stivers, R. 2004. Shades of Loneliness: Pathologies of a Technological Society. Lanham: Rowman & Littlefield Publishers, Inc.

Strathern, M., ed. 2000. Audit Cultures: Anthropological Studies in Accountability, Ethics and the Academy. London: Routledge.

Sutter, K. 2008-2014. Sons of Anarchy. United States: 20th Television.

Swyngedouw, E. 2018. Promises of the Political: Insurgent Cities in a Post-Political Environment. Cambridge, Massachusetts: MIT Press.
https://doi.org/10.7551/mitpress/10668.001.0001

Thompson, H. S. 2012. Hell's Angels: A Strange and Terrible Saga. New York: Ballantine Books.

Thompson, W. E. 2008. 'Pseudo-Deviance and the 'New Biker' Subculture: Hogs, Blogs, Leathers, and Lattes.' Deviant Behavior 30 (1): 89-114.
https://doi.org/10.1080/01639620802050098

Todolí-Signes, A. 2019. 'Algorithms, artificial intelligence and automated decisions concerning workers and the risks of discrimination: the necessary collec-

tive governance of data protection.' Transfer 25 (4): 465-481. https://doi.org/10.1177/1024258919876416

Valentine, S. 2019. 'Impoverished Algorithms: Misguided Governmnents, Flawed Technologies, and Social Control.' Fordham Urban Law Review 46 (2): 364-427.

Verkaaik, O. 2004. 'Purity and Transgression: Sacred Violence and the Quest for Authenticity.' Etnofoor 17 (1/2): 44-57.

Wahl-Jorgensen, K., L. K. Bennett, and J. Cable. 2016. 'Surveillance Normalization and Critique.' Digital Journalism. https://doi.org/10.1080/21670811.2016.1250607

Weiner, A. B. 1992. Inalienable Possessions: The Paradox of Keeping-while-giving. Berkeley: University of California Press. https://doi.org/10.1525/california/9780520076037.001.0001

Whelan, A. 2013. 'First as Tragedy, then as Corpse.' In Zombies in the Academy: Living Death in the Higher Education, edited by Andrew Whelan, Ruth Walker and Christopher Moore, 11-26. Bristol: Intellect.

Yang, K.-C., O. Varol, C. A. Davis, E. Ferrara, A. Flammini, and F. Menczer. 2019. 'Arming the Public with Artificial Intelligence to Counter Social Bots.' Human Behavior and Emerging Technologies 1: 48-61. https://doi.org/10.1002/hbe2.115

Zuboff, S. 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. London: Profile Books.